Title: Challenges to Ensuring Secure .COM and .EDU Access to a Web-based Air Force Laboratory Program Management

Track: Information Superiority/Information Operations

Authors: Helen M. Rico
Fred Hall
Francesca Paugh
Jacqueline Smith
Frank Born
Wayne Bosco

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Challenges to Ensuring Secure .COM and .EDU Access to a Web-based Air Force Laboratory Program Management	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Laboratory,AFRL/IFGA,525 Brooks Road,Rome,NY,13441**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**22**	

Challenges to Ensuring Secure .COM and .EDU Access to a Web-based Air Force Laboratory Program Management

Authors: **Helen M. Rico**
Air Force Research Laboratory/ Information Directorate
AFRL/IFGA
525 Brooks Road
Rome, New York 13441
315-330-3432 (phone)
315-330-1995 (fax)
Helen.Rico@rl.af.mil

Fred Hall
Air Force Research Laboratory/ Information Directorate
AFRL/IFGA
525 Brooks Road
Rome, New York 13441
315-330-2306(phone)
315-330-1995 (fax)
Fred.Hall@rl.af.mil

Francesca Paugh
Air Force Research Laboratory/ Information Directorate
AFRL/IFGA
525 Brooks Road
Rome, New York 13441
315-330-2910 (phone)
315-330-1995 (fax)
Francesca.Paugh@rl.af.mil

Jacqueline Smith
Air Force Research Laboratory/ Information Directorate
AFRL/IFGA
525 Brooks Road
Rome, New York 13441
315-330-2130 (phone)
315-330-1995 (fax)
Jacqueline.Smith@rl.af.mil

Frank Born
Air Force Research Laboratory/ Information Directorate
AFRL/IFTB
525 Brooks Road
Rome, New York 13441
315-330-4726(phone)
315-330-1995 (fax)
Frank.Born@rl.af.mil

Wayne Bosco
Air Force Research Laboratory/ Information Directorate
AFRL/IFTB
525 Brooks Road
Rome, New York 13441
315-330-3578 (phone)
315-330-1995 (fax)
Wayne,Bosco@rl.af.mil

Abstract

Timely, accurate, and secure information is essential to the Air Force Research Laboratory (AFRL), Information Directorate (IF), Rome, New York, whose mission is to provide superior information systems in support of the war fighter. With such information, improved decisions can be made regarding financial, acquisition, and personnel matters. In this paper the authors describe an automated Program Management capability newly deployed for use by all scientists, engineers, contracting, financial and management personnel working at the Air Force Research Laboratory, Information Directorate. It is important to recognize, the application currently has over 66% of its users logging into a .mil network from a .com or .edu world. Security is a significant factor that must be considered when allowing users outside of a .mil environment to access this Program Management System. Moreover, current Department of Defense (DoD) and Air Force (AF) regulations do not adequately address this new environment. This paper will describe the Program Management System and the local procedures implemented to ensure the system remains secure and the challenges associated with the effort. Additionally, this paper will include a description of user's roles and responsibility, how access is granted, the traceability aspect of the system, and finally sustainment issues.

Access Requirements to the AFRL Program Management System and Application

A distinction needs to be made between the web based Program Management application and the overall Program Management system. The system contains processes, and protects the data and code. There are many users that access the application, however, there are only a few users who have access rights into the AFRL Program Management System. Users having access to the system include the developers, system administrators, database administrators, and security managers. Each of these individuals has completed or has submitted a National Agency Check (NAC) prior to having been granted a system or administrator based account.

The AFRL Program Management System consists of a Web Based application which provides the front-end access into an Oracle database and uploaded documents via the web pages. It supports Secure Socket Layers and 128 bit encryption.

Classification of the system:

The highest classification of the AFRL Program Management System's database is unclassified. However it does contain sensitive data to include For Official Use Only (FOUO) and Proprietary data. The database does not retain Privacy Act regulated data.

Profile of the application users:

- 33% Government employees (Civilian and Military) and on-site contractor support staff (who have already been granted access to .mil or .gov network services).

- 66% Non-government personnel (i.e. contractors from outside of the .mil and .gov domain) to include universities and off-site contractors.

- <1% Foreign Nationals who fall within authorized US Government programs as outlined in AFI 33-202 Computer Security Paragraph 3.7, Requirements for Foreign National Access to Unclassified but Sensitive Internet Protocol Router Network (NIPRNet).

All users are required to be citizens of the United States of America or hold a valid Permanent Resident Card (I-551). Approval for Foreign National Access must follow Table 3.1 "Approving Authority for Foreign National Access" as provided in AFI33-202.

Application Account Generation:

The process for authorizing and activating accounts into the application is a multi-phased approach. The driving force for this process is due to the fact greater than 66% of the users will never be physically seen by on-site administrative personnel.

1) An existing user must "nominate" a person for an application account by entering the individual's name against a specific position within an existing Program or Project.

2) The System will automatically generate a Confirmation Code which is supplied to the "Nominator".

3) The "Nominator" must contact the "Nominee" either in person or by phone, to pass the Confirmation Number and the phone number of the Help Desk.

4) The "Nominee" must call or visit the Help Desk to provide identification and the confirmation number.

5) If the information provided matches, the Help Desk personnel will immediately generate the "nominee's" login and a temporary password. This information is given to the "nominee" along with the System's URL.

6) Upon the first login, the nominee will be forced to change the temporary password to proceed to access the system.

7) The nominee must fill out information equivalent to an electronic visit request and obtain appropriate security signatures. This information includes citizenship

information and the nominee's signatures indicating the nominee will follow appropriate security awareness practices.

8) Once the nominee prints the completed Agreement Document, the nominee must obtain all appropriate signatures and is required to fax the User Agreement to the Help Desk.

9) The Help Desk will review the Agreement Document for completeness.

10) If the information is accurate, the Help Desk activates the user as an active account. If the information is inaccurate, the help desk will resolve any discrepancy.

11) The help desk emails a notification to the nominee indicating the account has been activated.

Security Regulations:

Security is a major component for any new government software development effort. All software developed under this effort is required to comply with the list of the regulations identified below. These regulations, including the Department of Defense Directive (DoDD), Air Force Systems Security Instruction (AFSSI), Air Force Instruction (AFI), Air Force Manual (AFM), Air Force Material Command Supplement (AFMCS), and Air Force Directive (AFDIR) must be reviewed. Each regulation has a specific purpose which describes the government's point of view regarding software development and levels of risk. The paragraphs identified below address the most relevant issues for this paper.

Regulation	Series	Title	Date	Paragraph(s)
DODD 8500.2		Information Assurance (IA) Implementation	6 Feb 2003	E2.1.51. Sensitive Information. E2.1.51.1. For Official Use Only (FOUO). E2.1.51.4. Unclassified Technical Data. E2.1.51.5. Proprietary Information.
AFI 33-202	Communications and Information	Computer Security	30 Aug 2001	3.6. Multi-User Information Systems. "This section applies to all multi-user file servers (e.g., file transfer protocol [FTP]), network file servers, World Wide Web servers, etc.)…" 3.6.1. Unclassified and Sensitive Processing…. 3.7. Requirements for Foreign National Access to Unclassified But Sensitive Internet Protocol Router Network (NIPRNet).
AFI33-202/ AFMCS 1	Communications and Information	Computer Security	21 May 2002	3.19. Account, Login, and Password Management
AFM 33-223	Communications and Information	Identification and Authentication	1 Jun 1999	3.6. Password Change Authorization. Chapter 4 Identification and Authentication Maintenance and

				Management Responsibilities 4.3. Deleting User Accounts and Passwords. 4.4. Maintaining User Accounts. 4.5. System Configuration. 4.6. Audit Trails.
AFM 33-223/ AFMCS 1	Communications and Information	Identification and Authentication	24 Mar 1999	Entire supplement is applicable
AFI33-332	Communications and Information	Air Force Privacy Act	8 Nov 2000	Entire instruction is applicable
AFSSI 5027	Communications and Information	Network Security Policy	27 Feb 1998	5.2. Identification and Authentication 6.18. HTTP services

Table 1: Security Regulations

In addition to following regulations, there are several components that have been addressed to ensure the system meets the required security requirements. Each component will be discussed below:

Application Software Security: Security of the application is paramount to the security of the system. Application code that is insecure will negate all the efforts to lock down the hardware, operating system, web server and database. The Program Management System application software utilizes compartmental information, multiple permission levels, page level checks of those permission levels, and strong passwords to achieve the security of the information system. It also relies on delegation of permission assignment authority to ensure that the correct people have access to the information that they require.

Compartmental Information structure: A substantial portion of the work at the Air Force Research Laboratory involves "Project" management. These projects can be in-house research or contracts with corporations, small businesses or universities. Projects can be individual efforts, or be part of a large group of contracts and in-house research that comprise a much bigger "Program".

Programs

Overview Pages: Current rules for publicly available government web sites do not allow personal names or email addresses to be included in the site. This and other restrictions applied to the public sites make it difficult to share meaningful data to trusted parties who have a legitimate interest in a program. Several programs in the Program Management System contain overview pages that provide a password protected environment for sharing data about that program. These pages are a combination of hard coded HTML and ties to the database data. The permission level that is required for users to proceed beyond these pages can also be specified in the code for the page. Often tools available within the Program Management System such as document sharing capability or program calendar are linked through these upfront pages.

Collaboration Enabled: When projects are part of a bigger program there is often a requirement for them to work together. To enable this, the Program Management System team has created a number of collaboration tools that can enable collaboration. When collaboration is enabled, contractors will have a window into a defined portion of the project data for other projects in this program. Some of these items include project objectives, schedule, progress notes, papers and presentations. They will also be able to share data through the program calendar and message board.

Collaboration Disabled: When collaboration is disabled for a program there is no need for contractors to know that each other exist. The government personnel can still use the program calendars, message board etc and have limited access to data about other projects (that they do not own) in that program.

Projects

Financial data: Most of the financial data in the Program Management System is extracted directly from the corporate database. Contractors are instructed to enter monthly spending figures (accrued value) and also to identify their future funding profile as necessary. This data is only shared with the government and contractors who are identified as part of that project.

Technical Data: Technical data in the Program Management System generally comes from the contractor entering their monthly or quarterly status reports, or government engineers entering contractual data such as project objectives and schedules.

Page Security: Page security takes multiple forms in AFRL's Program Management System's application.

Permission Checks: Each page within the application performs permission checks. Each page checks for the user's permission level within the program that they are currently accessing. This permission level may be further qualified by the data access privileges that the user has for the project identified on that page. Permission errors automatically generate an email to the Program Management System development team. The team can evaluate if there is an error in the application that caused the permission error, or if it is a deliberate attempt to hack the application code.

Disabled URL Editing: In addition to page level permission checks, there is also a prohibition on editing the URL (address) of the web page. This will disallow the user from logging into one area and trying to access data in another area (or program or project etc). As with permission checks, url editing permission errors

automatically generate an email to the Program Management System development team.

Tailored Navigation Bars: AFRL's Program Management System front-end application tailors the navigation bar based on the user's permission level and the program that they are currently accessing. As such, users will not have links to pages that they have no permission to access. However, if a user should find such a link, they would be stopped at the page level permission check.

Multi-tiered Permission Structure: There are currently approximately 50 "Programs" contained within the database. Permissions that are assigned to a user are assigned for a specific program and are only applicable for that program (the exception is the "Program Management System Admin" permission level and the "Help Desk" permission level). Users may have different permission levels in different programs.

- ***Program Management System Admin*:** This is a system level account. This permission allows users to access and edit all the data in the Program Management System (except that which is extracted from the corporate data feed). The user also has access to the management pages in the system for creating and rearranging programs, projects, and people.

The following are application level accounts:

- ***Help Desk:*** This permission is reserved for help personnel to assign login names and temporary passwords, lock and unlock accounts, and edit user data.

- ***Super User:*** This person can see and edit (almost) all data associated with the particular program except that which comes from other corporate databases. These users are responsible for user accounts and project additions/deletions in a program.

- ***AllProjects:*** This person can see (but not edit) most data associated with the particular program. Typically, this permission level is for Program Managers or their support personnel.

- ***OwnProject Government:*** This person has rights to see and edit most of the data pertaining to those projects that they are listed as a Point of Contact (POC) in a particular program. They are also able to see "public" information from the other projects in the program.

- ***OwnProject Contractor:*** This person has rights to see and edit some data pertaining to those projects that they are listed as a contractor POC in a particular program. If that program has the collaboration

tools enabled, the person will also be able to see "public" information from other projects in the program.

- ***All Projects No Financials:*** This category of permission level is used in two separate instances. The first is for a domain expert who would need to see all the collaboration information, but would not need to see financial information (or private portions of status reports) for any of the projects. The second case where this permission level would be used is for a researcher who is identified as an "Other Technical" POC for a project but is not given access to view financial information for that (or other) projects.

- ***ViewOnly****:* This person will only be able to see a limited set of information within the application. This includes some documents and some "public" information. The users are generally not given access to the navigation banner or its pages.

Password Security: Password security is an important part of our overall system security. The password security measures are in accordance with AFMAN 33-223 (paragraphs 2.4 and 2.6 of the original and the AFMC supplement) and AFI33-202 AFMC Supplement 1 (paragraph 3.19). The following is a list of the current security measures:

- ***Encryption:*** All passwords contained in the database are encrypted. Transmission of all data is encrypted.

- ***Strength:*** Password strength follows the same information assurance standards that are required for AFRL/IF's network access.

- ***Expiration, Limited Frequency of Change:*** Passwords are forced to be changed on a regular basis, but can not be changed more frequently than a set number of days.

- ***Limited Reuse:*** New Passwords can not match the ten previous passwords.

- ***Forced Change****:* In the event of security concern, all users can be forced to change their password upon next login.

Delegated Authority: Due to the fact the application is used by both government and contractors, there is no possibility for the help desk to know who should have permissions in the system and at what level. As such, the authority to set up permissions in the system is delegated down to a valid application user and only within their particular "Program" or "Project". Users are urged to continually check, and update as necessary, the list of those who have permissions to access the data on their projects. The

only level of permission that is not delegated to users to assign is the super user permission level. The super user permission level can only be assigned by the help desk.

- ***Contractors:*** Contractors who are listed as a POC for a specific contract have the ability to grant other contractors access to their project (at the same permission level or lower).

- ***Government POCs:*** Government personnel who are listed as a POC for a specific contract have delegated authority to grant access to other government POCs for that contract at the government POC permission level. They are also allowed to assign contractors POC's at either of the contractor POC permission levels. Government POC's can grant access to individuals at the "View Only" permission level.

- ***Local Super Users:*** Super users have read and edit access to almost all data in the Program Management System program (group of contracts, grants etc). As such they can add users as a government or contractor POC on any project in that program; they can add personnel at the "All Projects" or "View Only" permission level.

- ***Automatic Permission Assignments:*** In most cases, when users are granted access to a portion of the application they are automatically assigned the correct permission level by the system. For instance, in most of the cases listed above, when a user assigns someone as a POC for a particular project they do not also have to assign an appropriate permission. The Program Management System will do that automatically. In the case of contractor POCs being assigned to a project, the user must select whether this person requires access to the financial data for the project. The Program Management System will use this data to grant the appropriate permission level to that person.

User Agreement Document: As described earlier, all users are required to complete a user agreement document prior to being granted an account within the application. This document is used to verify the individual is a US citizen or a Permanent Resident Alien, and to obtain the individual's acknowledgement which states the user will abide by certain rules when accessing the application.

Filename security (obscurity): Documents uploaded to the system are currently stored in the file system of the web server. As such, there was a need to make those addresses impossible to guess by outsiders trying to hack the system. Therefore, a password strength string was added to each of the filenames.

Session Variables:

Server Based Authentication: All authentications of user accounts and access permissions are done at the server using session variables. If the user has proper

permissions for the page the server will send the correct set of data to the browser. If the user somehow reached the page but did not have the correct permission level, a permission error will be generated and no data will be sent to the browser.

Session Timeout: Timeouts within the application help keep users from piggybacking on another's open session. They also enable the system to free up memory space when the user logs out or closes their browser.

System Traceability: There are multiple places where a user can be nominated or assigned as a POC in the application. There is a requirement to track who performed the associations and the types of actions. Every user has a unique identifier called user-ID which is utilized within the traceability code.

A traceability module was added to the Program Management System. This code allows for audit trails to be generated with respect to changes made to accounts. Guidance for this module was taken from AFMAN 33-223 (paragraph 4.6) and its AFMC supplement. Traceability includes:

- Identification of the person responsible for entering a user into the system (nominator).
- Identification of the person responsible for associating a user with a program or project.
- Identification of the person responsible for locking a user account.
- Identification of the person responsible for changing a user's permission level (includes removal from a program or project).
- Time/Date-stamp all "person responsible" transactions.

Sustainment: Account maintenance is accomplished regularly to ensure the system is adequately protected against hackers. Reference AFMAN33-223 and its AFMC supplement (Paragraphs 4.3 and 4.4), AFI33-202/AFMCS 1 (paragraph 3.19.6), and AFRL/IF policy:

- For users leaving the AFRL/IF: User-IDs and passwords are locked by close of business one day following the user's departure.
- The Contractor Principal Investigators are instructed to remove users from the internal Points of Contact list upon departure from their organization. The Contractor Principal Investigator must notify the Government Program Manager regarding the change.

- Accounts are reviewed every six months to determine dormant user-IDs and passwords.

- User's authorization is revalidated annually at a minimum. Program and Project managers are encouraged to revalidate the Points of Contact lists associated with their programs and projects as needed but required by regulation to perform the revalidation process annually.

Benefits: As a result of creating a new Program Management System the flow of information is more rapid, Government mandates to reduce the amount of paperwork generated are adhered to and cost savings can be achieved. The new application streamlines the previous program management reporting process by eliminating redundant manual entry. Additionally, it allows users from a .com or .edu environment to access a .mil system to upload documents or enter data.

In summary, the system improves managers' efficiency and provides an on-line repository for all information associated with a contract, as well as providing users outside of the government a window into this system to view and enter their data while adhering to all security requirements.

Challenges to Ensuring Secure Dot-COM and Dot-EDU Web Access

June 19, 2003

Standards-Based Architecture Program Office

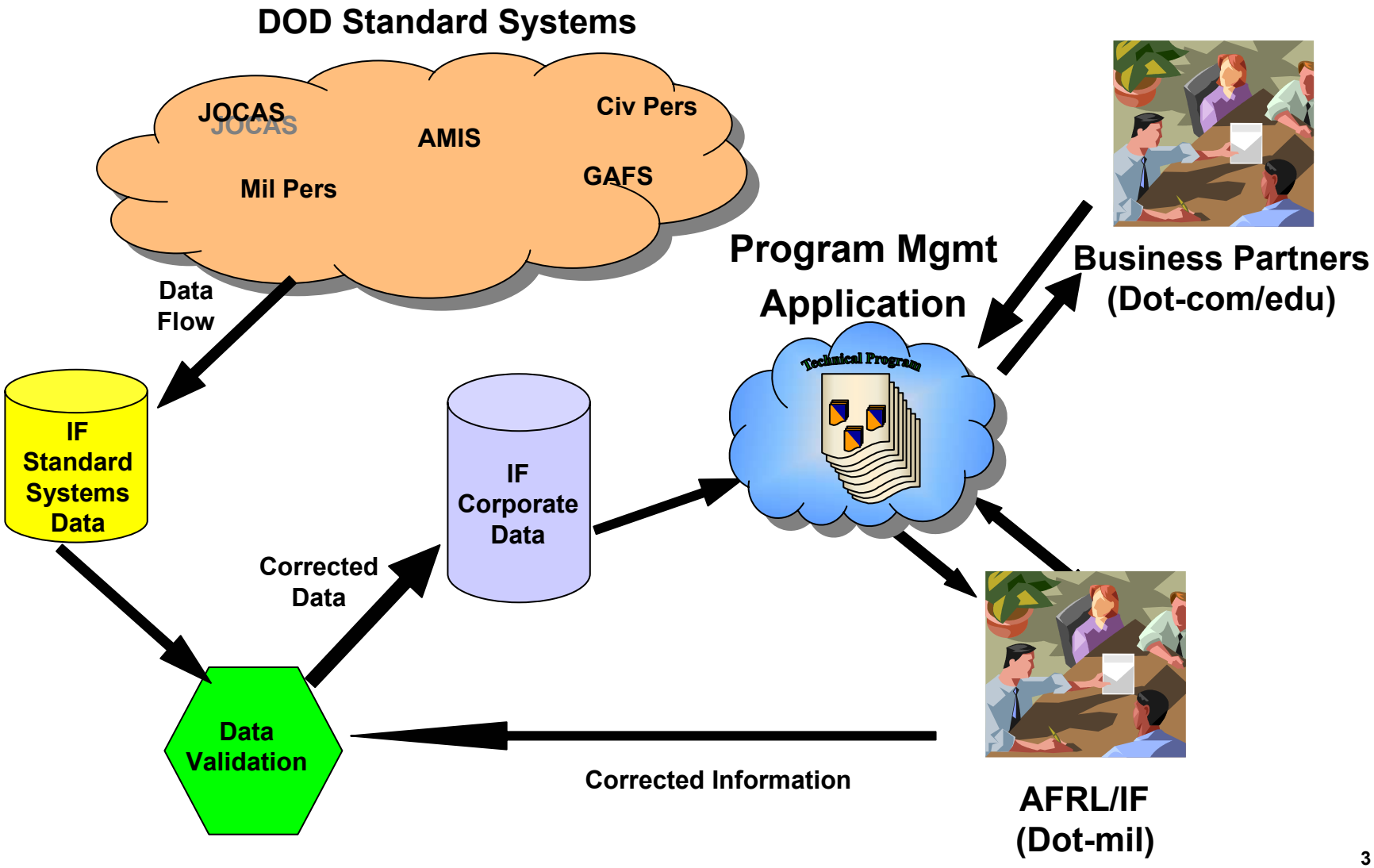
Information Directorate

Air Force Research Laboratory

System Information

- Web Based Tool Built Primarily for Post Award Contract Management
- Designed for a Distributed Work Environment
- Contractor Financial and Technical Reporting
- Government Sharing of Program Management Info
- One Way Data Feeds from Corporate Database (Data Entered Once)
- Data entry is almost entirely web based and validated against AFRL corporate data
- Goal is to make contract reporting quick and easy and provide access to needed effort or program information.

Information Strategy

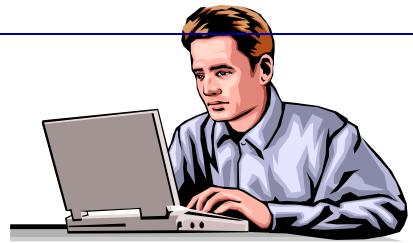


Tailored User Information

Dot-mil Users

Dot-com/edu Users

Buyer



LPM

LPM Support

Super User

Financial Administrator

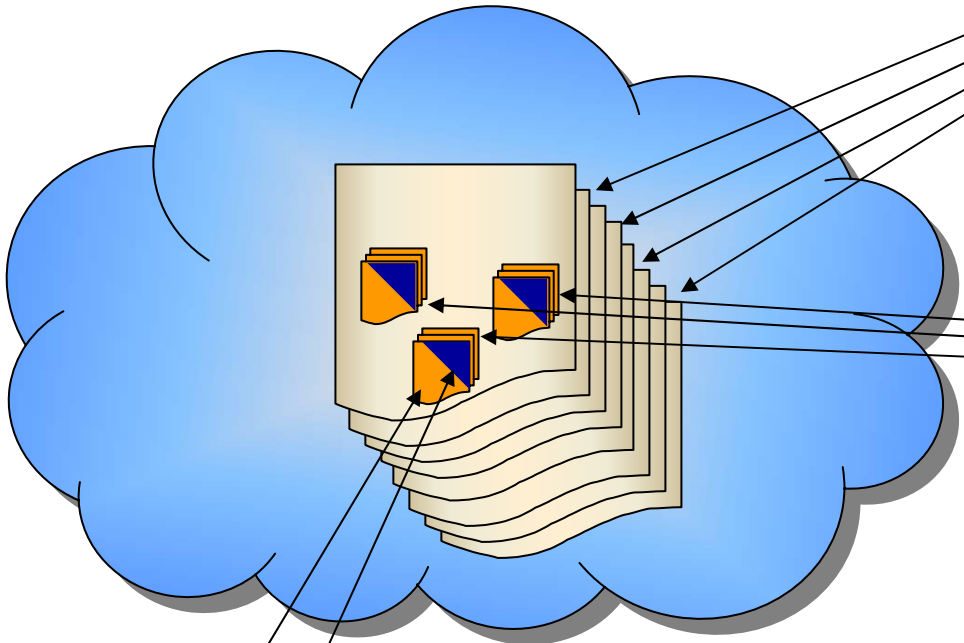
Other Technical

Principal Investigator (PI)

PI Support

Data Compartmenting

- **Application accounts are limited by the User's Programs, Projects And Permission Level.**



Programs

- Collaboration
- Non-collaboration

Projects

- Contracts
- In-House
- Working Groups

Data Access

- Government Only
- Govt and Contractor

Permission Levels

- 5 possible levels

User Management

- User Agreements
  - Verify identity
  - Agree to Rules
- Secure Passwords
- Delegated Authority
  - Local Super Users
  - Govt POCs
  - Contractor POCs
- Automatic Permission Assignments
- Audit Trails
  - User Traceability
  - Security Reports

Add / Edit

All Program Functions/People

All Project Functions/People

Some Project Functions/People

Who did What to Whom and When

and

Who can see What since When

Account Generation Procedure

Existing App user

Nominates person

System generates Confirmation Code for new account

Confirmation Code given to Nominee

Verbal Identification and Confirmation Code given to Help Desk

Nominee

Login and change temporary password

Begin Using System

Fill out electronic Account Agreement

Print out, get signatures, fax Account Agreement to Help Desk

Help Desk

User ID, Temporary Password, System URL sent to Nominee

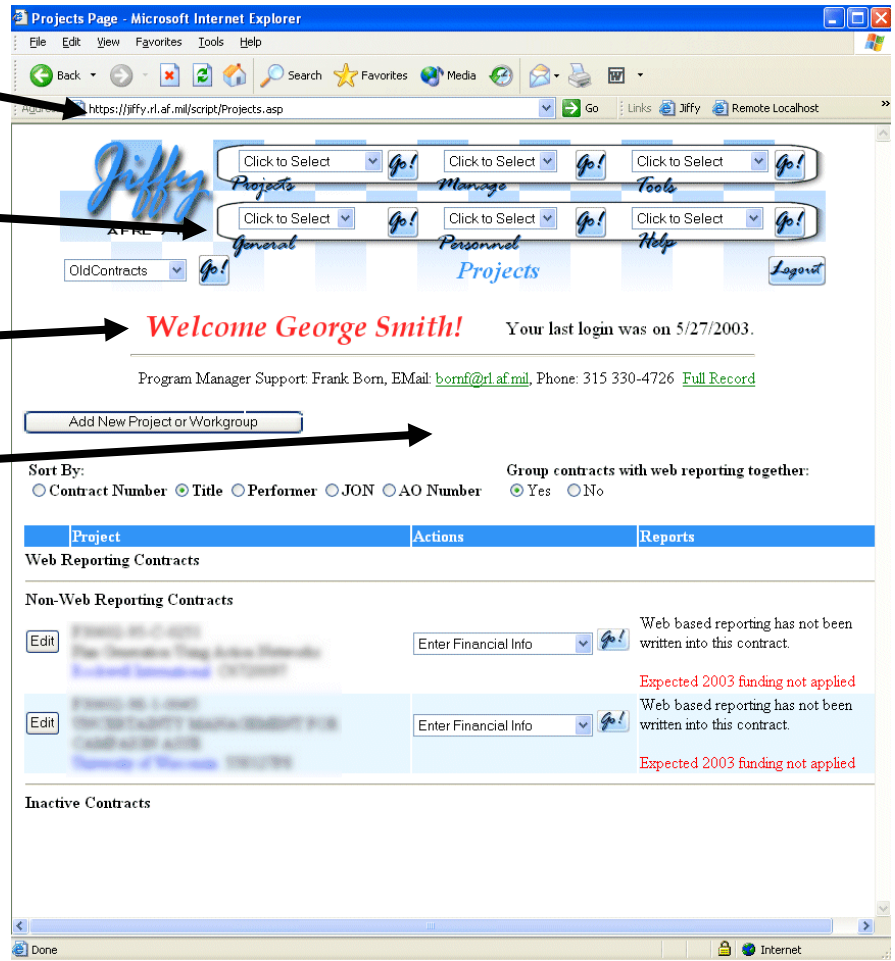
Email Notification of Valid User Account Creation to Nominee

Review Account Agreement

Activate User Account

Page Security

- Disabled URL editing
- Permission Level / Program Tailored Navigation Bars
- Server based User Authentication
- Page Level Permission Checks
- Session Timeouts
- Session Logout



Additional Security Measures

- Web server not a member of the domain
- Secure Socket Layer
- 128 bit encryption
- File name obscurity

https://PMSys.af.mil/Documents/Program/DCF10/ISI_2-0576(Le+G1Rpvvic2T)7.htm